



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/732,954	12/07/2000	Michael Wray	B-4053 618409-8	2785

7590 01/28/2005

HEWLETT-PACKARD COMPANY  
INTELLECTUAL PROPERTY ADMINISTRATION  
P.O. BOX 272400  
3404 E. HARMONY ROAD  
FORT COLLINS, CO 80527-2400

EXAMINER

NALVEN, ANDREW L

ART UNIT PAPER NUMBER

2134

DATE MAILED: 01/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/732,954	WRAY, MICHAEL	
	<b>Examiner</b>	<b>Art Unit</b>	
	Andrew L Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 27 July 2004.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-36 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 07 December 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>July 20, 2004</u> . | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. Claims 1-36 are pending.

### ***Response to Arguments***

2. Applicant's arguments filed 27 July 2004 have been fully considered but they are not persuasive.

3. Applicant has argued on Pages 15 and 16 that the Menezes reference "The Book of Applied Cryptography," fails to teach the step of seeking a backwards proof of said primary goal as represented by item b of claim 1. Examiner respectfully disagrees. Menezes teaches a system of verification (proof) by the creation of a certificate chain from reverse certificates so as to start at a bottom or root node and move up towards a certificate authority (Menezes, Page 573, Example 13.42, Page 575). Examiner contends that Menezes teaches the seeking of a backwards proof of the primary goal by a process of recursively taking a goal to be proved, starting with the primary goal, decomposing it into subgoals (Menezes, Page 573, Section iii, subgoal viewed as cross certificate as a portion of a method of verifying) one of which corresponds to an attribute delegation that is justified by an available certificate and has the same subject as the goal being decomposed, inability to decompose a subgoal that has not been proved causing the process to backtrack to a previous subgoal to seek a new decomposition

Art Unit: 2134

(Menezes, Page 575, Section 13.6.2 Part 4, Page 572-573 Section 13.6.2 Part 1, depth first or breadth first search).

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot et al US Patent No 6,134,550 in view of The Book of Applied Cryptography by Menezes et al.

6. With regards to claims 1, 13, and 25, Van Oorschot teaches the setting as a primary goal to be proved an attribute delegation from a known trusted issuer to a subject (Van Oorschot, column 12 lines 6-7, column 5 lines 15-25, column 8 lines 43-48) and the determining that a trust chain has been found by producing a chain of sub-goals proved by corresponding certificates (Van Oorschot, column 12 lines 14-18) that grounds in a sub-goal justified by a justified attribute delegation that has as issuer the known trusted issuer included in the primary goal (Van Oorschot, column 12 lines 8-25). Van Oorschot fails to teach the seeking of a backwards proof of the primary goal by recursively taking the goal to be proved and decomposing it into subgoals. Van Oorschot fails to teach the seeking of a backwards proof. Menezes teaches the seeking

of a backwards proof of the primary goal by a process of recursively taking a goal to be proved, starting with the primary goal, decomposing it into subgoals one of which corresponds to an attribute delegation that is justified by an available certificate and has the same subject as the goal being decomposed, inability to decompose a subgoal that has not been proved causing the process to backtrack to a previous subgoal to seek a new decomposition (Menezes, Page 575, Section 13.6.2 Part 4, Page 572-573 Section 13.6.2 Part 1). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Menezes' method of using backtracking proofs because it offers the advantage of removing the need for a central trusted authority by providing a distributed trust model where any certificate authority may cross-certify any other (Menezes, Page 575, Section 13.6.2 Part 4).

7. With regards to claims 2, 14, and 26, Van Oorschot as modified teaches that the known trusted issuer included in the primary goal is a specifically identified entity that is inherently trusted by the discovery method at least in relation to the required attribute (Van Oorschot, column 4 lines 52-55) and that the justified attribute delegation is an attribute delegation that is justified by a corresponding certificate (Van Oorschot, column 12 lines 5-13).

8. With regards to claims 3, 15, and 27, Van Oorschot as modified teaches that the known trusted issuer included in the primary goal is the discovery method itself and the justified attribute delegation is an attribute delegation that is justified either by an axiom inherently trusted by the discovery method or by a corresponding certificate (Van Oorschot, column 11 lines 50-55).

Art Unit: 2134

9. With regards to claims 4, 16 and 28, Van Oorschot as modified teaches the discovery method as the known trusted issuer being represented in the primary goal and the axiom as a null issuer (Van Oorschot, column 11 lines 50-55 and lines 8-23).

10. With regards to claims 5, 17 and 29, Van Oorschot as modified teaches that name mappings justified by corresponding certificates are permitted in a trust chain in addition to attribute delegations, step (b) involving decomposing a particular subgoal to be proved into a name mapping justified by an available certificate and a new subgoal corresponding to the particular subgoal but with the subject reverse mapped using the name mapping (Menezes, Page 575, Section 13.6.2 Part 4).

11. With regards to claims 6, 18, and 30, Van Oorschot as modified teaches the maintaining of a list of subgoals already pursued, checking each new subgoal against the list, terminating the process of step (b) in failure in the event a new subgoal is already in the list (Van Oorschot, column 7 lines 17-34, column 10 lines 55-58, Menezes, Page 575, Section 13.6.2 Part 4).

12. With regards to claims 7, 19, and 31, Van Oorschot as modified teaches the certificates having validity data and the forward traversing of the trust chain to determine the validity of the overall attribute delegation represented by the chain (Van Oorschot, column 11 line 61 – column 12 line 5).

13. With regards to claims 8, 20, and 32, Van Oorschot as modified teaches the storing of the state of the process prior to checking the validity of the trust chain found such that the state could be used to continue the process should the check of the validity fail (Van Oorschot, column 12 lines 14-18).

Art Unit: 2134

14. With regards to claims 9, 21, and 33, Van Oorschot as modified teaches that the attribute-delegation certificate used to prove the subgoal has a subject-directed condition associated with it requiring that a specific subject must have a particular attribute in order for the delegation to be valid and this condition is a further subgoal to be proved (Van Oorschot, column 4 lines 52-62).

15. With regards to claims 10, 22, and 34, Van Oorschot as modified teaches the process of step (b) running to completion to find all trust chains, if any, proving the primary goal (Van Oorschot, column 10 lines 35-55, column 12 lines 14-18).

16. With regards to claims 11, 23, and 35, Van Oorschot as modified teaches the selecting of certificates to be sent to a resource that requires proof that a subject has a particular attribute before allowing use of the resource (Van Oorschot, column 12 lines 20-40).

17. With regards to claim 12, 24, and 36, Van Oorschot as modified teaches the determining that the use of the resource is permitted if a trust chain can be found (Van Oorschot, column 10 lines 35-58, column 12 lines 6-11).

### ***Conclusion***

18. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2134

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571 272 3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

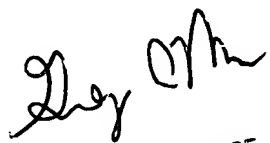


Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

AN

  
GREGORY MORCE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100